

## **AMENDMENTS TO THE CLAIMS**

This listing of claims will replace all prior versions, and listings, of claims in the application:

### **Listing of Claims:**

- 1           1. (Currently amended) A method for facilitating the delegation of  
2           operations involved in providing digital signatures to a signature server, the  
3           method comprising:  
4           |       allowing a user to authenticate the signature server prior to sending a  
5           |       message to the signature server;  
6           |       receiving a the message from a the user at the signature server, the  
7           message including an item to be signed on behalf of the user by the signature  
8           server;  
9           looking up a private key for the user at the signature server; and  
10          signing the item with the private key for the user.
  
- 1           2. (Original) The method of claim 1, wherein prior to signing the item, the  
2           method further comprises authenticating the user.
  
- 1           3. (Original) The method of claim 2, wherein prior to signing the item, the  
2           method further comprises determining whether the user is authorized to sign the  
3           item.
  
- 1           4. (Original) The method of claim 3, wherein determining whether the user  
2           is authorized to sign the item involves looking up an authorization for the user

3 based upon an identifier for the user as well as an identifier for an application to  
4 which the user will send the signed item.

1 5. (Original) The method of claim 3, wherein determining whether the user  
2 is authorized to sign the item involves communicating with an authority server  
3 that is separate from the signature server.

1 6 (Canceled).

1 7. (Previously presented) The method of claim 1, further comprising  
2 returning the signed item to the user so that the user can send the signed item to a  
3 recipient.

1 8. (Original) The method of claim 1, wherein the method further  
2 comprises configuring the signature server to accommodate a new user by:  
3 receiving a request from an authorized entity to add the new user;  
4 generating a key pair for the new user, including a new user private key  
5 and a new user public key;  
6 communicating with a certification authority to obtain a certificate for the  
7 new user based on the key pair; and  
8 storing the certificate and the key pair for the new user in a location that is  
9 accessible by the signature server to enable the signature server to sign items on  
10 behalf of the new user.

1 9. (Original) The method of claim 1, wherein the method further  
2 comprises configuring the signature server to delete an old user by:  
3 receiving a request from an authorized entity to delete the old user;

4 notifying a certification authority to revoke a certificate for the old user;  
5 and  
6 removing the private key for the old user from the signature server, so that  
7 the signature server can no longer sign items on behalf of the old user.

1 10. (Previously presented) The method of claim 1, wherein the method  
2 further comprises archiving the message and the signed item at the signature  
3 server.

1 11. (Original) The method of claim 1, wherein the method further  
2 comprises forwarding the signed item to an archive server in order to be archived.

1 12. (Canceled) A computer-readable storage medium storing instructions  
2 that when executed by a computer cause the computer to perform a method for  
3 facilitating the delegation of operations involved in providing digital signatures to  
4 a signature server, the method comprising:  
5 allowing a user to authenticate the signature server prior to sending a  
6 message to the signature server;  
7 receiving a the message from a the user at the signature server, the  
8 message including an item to be signed on behalf of the user by the signature  
9 server;  
10 looking up a private key for the user at the signature server; and  
11 signing the item with the private key for the user.

1 13. (Original) The computer-readable storage medium of claim 12,  
2 wherein prior to signing the item, the method further comprises authenticating the  
3 user.

1           14. (Original) The computer-readable storage medium of claim 13,  
2 wherein prior to signing the item, the method further comprises determining  
3 whether the user is authorized to sign the item.

1           15. (Original) The computer-readable storage medium of claim 14,  
2 wherein determining whether the user is authorized to sign the item involves  
3 looking up an authorization for the user based upon an identifier for the user as  
4 well as an identifier for an application to which the user will send the signed item.

1           16. (Original) The computer-readable storage medium of claim 14,  
2 wherein determining whether the user is authorized to sign the item involves  
3 communicating with an authority server that is separate from the signature server.

1           17 (Canceled).

1           18. (Previously presented) The computer-readable storage medium of  
2 claim 12, wherein the method further comprises returning the signed item to the  
3 user so that the user can send the signed item to a recipient.

1           19. (Original) The computer-readable storage medium of claim 12,  
2 wherein the method further comprises configuring the signature server to  
3 accommodate a new user by:  
4           receiving a request from an authorized entity to add the new user;  
5           generating a key pair for the new user, including a new user private key  
6 and a new user public key;  
7           communicating with a certification authority to obtain a certificate for the  
8 new user based on the key pair; and

9 storing the certificate and the key pair for the new user in a location that is  
10 accessible by the signature server to enable the signature server to sign items on  
11 behalf of the new user.

1 20. (Original) The computer-readable storage medium of claim 12,  
2 wherein the method further comprises configuring the signature server to delete an  
3 old user by:

4 receiving a request from an authorized entity to delete the old user;  
5 notifying a certification authority to revoke a certificate for the old user;  
6 and  
7 removing the private key for the old user from the signature server, so that  
8 the signature server can no longer sign items on behalf of the old user.

1 21. (Previously presented) The computer-readable storage medium of  
2 claim 12, wherein the method further comprises archiving the message and the  
3 signed item at the signature server.

1 22. (Original) The computer-readable storage medium of claim 12,  
2 wherein the method further comprises forwarding the signed item to an archive  
3 server in order to be archived.

1 23. (Currently amended) An apparatus that facilitates delegating  
2 operations involved in providing digital signatures, comprising:  
3 a signature server;  
4 an authentication mechanism that is configured to allow a user to  
5 authenticate the signature server prior to sending a message to the signature server

6 a receiving mechanism within the signature server that is configured to  
7 receive ~~a~~the message from ~~a~~the user, the message including an item to be signed  
8 on behalf of the user by the signature server;  
9 a lookup mechanism within the signature server that is configured to look  
10 up a private key for the user; and  
11 a signing mechanism within the signature server that is configured to sign  
12 the item with the private key for the user.

1 24. (Original) The apparatus of claim 23, further comprising an  
2 authentication mechanism that is configured to authenticate the user prior to  
3 signing the item.

1 25. (Original) The apparatus of claim 24, further comprising an  
2 authorization mechanism that is configured to determine whether the user is  
3 authorized to sign the item prior to signing the item.

1 26. (Original) The apparatus of claim 25, wherein the authorization  
2 mechanism is configured to determine whether the user is authorized to sign the  
3 item by looking up an authorization for the user based upon an identifier for the  
4 user as well as an identifier for an application to which the user will send the  
5 signed item.

1 27. (Original) The apparatus of claim 25, wherein the authorization  
2 mechanism is configured to determine whether the user is authorized to sign the  
3 item by communicating with an authority server that is separate from the signature  
4 server.

1 28 (Canceled).

1           29. (Previously presented) The apparatus of claim 23, further comprising a  
2 sending mechanism within the signature server that is configured to return the  
3 signed item to the user so that the user can send the signed item to a recipient.

1           30. (Original) The apparatus of claim 23, further comprising an  
2 initialization mechanism that is configured to:  
3           receive a request from an authorized entity to add a new user;  
4           generate a key pair for the new user, including a new user private key and  
5 a new user public key;  
6           communicate with a certification authority to obtain a certificate for the  
7 new user based on the key pair; and to  
8           store the certificate and the key pair for the new user in a location that is  
9 accessible by the signature server to enable the signature server to sign items on  
10 behalf of the new user.

1           31. (Original) The apparatus of claim 23, further comprising a deletion  
2 mechanism that is configured to:  
3           receive a request from an authorized entity to delete an old user;  
4           notify a certification authority to revoke a certificate for the old user; and  
5 to  
6           remove the private key for the old user from the signature server, so that  
7 the signature server can no longer sign items on behalf of the old user.

1           32. (Previously presented) The apparatus of claim 23, further comprising  
2 an archiving mechanism that is configured to archive the message and the signed  
3 item at the signature server.

1           33. (Original) The apparatus of claim 23, further comprising an archiving  
2 mechanism that is configured to forward the signed item to an archive server in  
3 order to be archived.